In re Appl. of Arditi et al.

Application No. 10/659,796

Response to Final Office Action of June 4, 2007

AMENDMENTS TO THE CLAIMS:

Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the

application:

Claim 1 (previously presented): A method for applying an electronic signature from a client

station, comprising the steps of: /A/ authenticating the client station at a server, thereby

establishing an authenticated communication channel between the client station and said

server; /B/ generating a private key/public key pair at the client station; /C/ sending from the

client station to the server, via the authenticated channel, a request for a signature certificate,

generated by means of at least the public key, said request providing to the server information

pertaining to at least the public key and excluding the private key; /D/ sending from the

server to the client station, via the authenticated channel, a signature certificate provided in

response to said request; /E/ calculating a cryptographic signature at the client station by

means of the private key, then destroying the private key at the client station; and /F/

formatting the calculated signature with the aid of the signature certificate received by the

client station via the authenticated channel.

Claim 2 (original): Method according to claim 1, wherein steps /C/ and /E/ are executed in

parallel at the client station.

Claim 3 (original): Method according to claim 1, wherein steps /B/, /C/, /E/ and /F/ are at

least partially executed at the client station under the control of a program downloaded from

2

In re Appl. of Arditi et al.

Application No. 10/659,796

Response to Final Office Action of June 4, 2007

the server in response to step /A/.

Claim 4 (original): Method according to claim 1, wherein step /A/ comprises mutually authenticating the server and the client station.

Claim 5 (original): Method according to claim 1, comprising the further step of verifying,

at the client station, the signature certificate received via the authenticated channel.

Claim 6 (original): Method according to claim 1, wherein the signature certificate obtained

by the server has a validity period of at most one day.

Claim 7 (original): Method according to claim 1, comprising the preliminary step of

registering the client station with respect to a certification authority with which the server

cooperates, or with respect to a registration authority associated with said certification

authority.

Claim 8 (previously presented): A computer program product on a recordable medium,

comprising instructions for controlling a client station having authentication resources with

respect to an electronic signature assistance server, said instructions including: instructions

for generating a private key/public key pair after the establishment of an authenticated

channel between the client station and said server; instructions for transmitting to the server,

via the authenticated channel, a request for a signature certificate generated by means of at

least the public key, said request providing to the server information pertaining to at least the

public key and excluding the private key; instructions for receiving from the server, via the

3

authenticated channel, a signature certificate obtained in response to said request; instructions for calculating a cryptographic signature by means of the private key, and then for destroying the private key; and instructions for formatting the calculated signature with the aid of the signature certificate received via the authenticated channel.

Claim 9 (original): Computer program product according to claim 8, wherein the instructions for transmitting the signature certificate request and the instructions for calculating the electronic signature and then for destroying the private key are executable in parallel.

Claim 10 (original): Computer program product according to claim 8, wherein at least some of said instructions form part of a program written in a mobile code language and downloadable from said server (2) after establishment of the authenticated channel.

Claim 11 (original): Computer program product according to claim 8, wherein said instructions further include instructions for verifying the signature certificate received via the authenticated channel.

Claim 12 (previously presented): An electronic signature assistance server, comprising means of authenticating a client station to establish an authenticated communication channel with said client station, means for obtaining a signature certificate in response to a request received from the client station via the authenticated channel and for transmitting said certificate to the client station via the authenticated channel, and means for downloading to the client station a program written in a mobile code language, including instructions for

controlling, at least partially, the execution of the following operations by the client station:

generation of a private key/public key pair at the client station after the establishment of the

authenticated channel; transmission to the server, via the authenticated channel, of a request

for a signature certificate generated by means of at least the public key, said request

providing to the server information pertaining to at least the public key and excluding the

private key; reception, via the authenticated channel, of the signature certificate transmitted

by the server in response to said request; calculation of a cryptographic signature at the client

station by means of the private key, followed by destruction of the private key; and

formatting of the calculated signature with the aid of the signature certificate received via the

authenticated channel.

Claim 13 (previously presented): An assistance server according to claim 12, wherein the

signature certificate has a validity period of at most one day.

Claim 14 (previously presented): An assistance server according to claim 12, wherein said

operations further comprise a verification of the signature certificate received via the

authenticated channel.

5